

HACKTIC

Uitgeverij van 'Winkeltekst' (Bla)

Met in dit eerste nummer.

- Computervirussen geknakt
- Colgate dicht geen gaten
- The Hacker Info System
- De internet worm
- Teleconferentie deel 1



Nederlands Grootste, Beste,
Voortelgste en Kinstrijkste
Hacker-blad

BACKTIC is Nederlandse eerste hackertblad. Maar we hopen verspreiden het ongeveer 10's per jaar.

HOOGTE met maats (ik heb een volkomen ongebonden en ongeorganiseerd gezelschap van vrienden typist).

REDACTIE: The Key, John D., T., Herman Acker, Peter Frederix en Rog.

ILLUSTRATES: Koen Hottentot.

CONTACT: De redactie is te bereiken via p.b. 32953, 1100 DL Amsterdam. Op VUCF via *Amsterdamsche*. Op het FIDO-net 3:28801 Hack Tic. Telex (nordens 20) laait telecommunicatieconferentie van de FTT) 12969 waakt al, telefax 808-74706. Zowel bij telex als bij fax even vermelden dat het voor Hack Tic is. Abonnees die er in slagen de redactie te bereiken (voelen) te bereiken moeten met vriendelijke afwijking houden.

FIJES: Lezer nummers kosten 4 gulden, een abonnement voor 10 nummers (ruist ongeveer een jaar meegaan) kost f 37,50. Abonnementen kunnen op bestelnummer 94.72.84.541 L.A. Rog Gorggip.

ERFALIC: Het is waar dat 'er' welken, hoe van je alleen maar met onze bestaatschietten in tijden om in deze van er abonnees zijn. Wij vinden Hack Tic een uitsluitend oorspronkelijk bladje, maar de kern bestaat dat lokale, regionale, nationale en in de toekomst wellicht zelfs Europese overheden het daar niet mee eens zijn. Het is een maatschappelijk te posten die je met wilt verspreiden dat kan je ook geld en soms tijd kosten in een overlopen die aan onze postbus sturen, wij weten dat ging om, dat is de post open maken kan je nog steeds de plaats. De Hack Tic wordt altijd verspreid in een nieuw teile envelop. (Streek denkt je hoopers nog dat je praatte koopje per postorder). Hack Tic is ook verkrijgbaar bij de goede boekhandel/juistheid heren/haar aan het overnemen voor de deur).

DECLAMER: Informatie is Hack/Tic doet slechts een educatief doel, Gebruik van deze informatie voor strafrechtelijke verantwoordelijkheid kunnen zijn. De redactie wijkt iedere verantwoordelijkheid voor gebruik door lezers van de in Hack/Tic opgenomen informatie af.

KADIEIC: Ingebruik Kanten, tijdschrift, onroepelingsen, politieke partijen, nieuwsmagazines, etc. etc. mogen zonder voorafgaande toestemming van de redactie (maar natuurlijk met betrouwen ding) rechten overnemen uit de Hack Tic. De bestaande afwijking blijft echter van kracht. Nadruk van de gehele Hack-Tic is natuurlijk verboden (zouwe toch maar een abonnement, want wij hebben het een heel veel goede adviezen die al welken met een ingetogen hebben).

HOE: Hack-Tic wordt met het WTCMWFYG (What You See Might Be What You Get) DTP pakket Versie 1.1 gemaakt op een gammale AT. Print ook van elke pagina gemaakt met een EPSON RX-80 en daarna veldteld en geïncalpeerd. Dat zeg een beetje d'r in en Maar wat Kien (hopen we terwijl we dit schreef)

IN DIT NUMMER	
1	Colofon & inhoud
2	Peter Frederix over Hack/Tic
3	Computersystemen A-dien C
4	WTCMWFYG
10	The Hacker's Ring System
12	Levenswijze
13	Collega getuigt
18	The Internet waar
20	Chess Computer Club
22	Chips Colofon, Gorggip '88
24	Back-up & volgende nummers

Hackers beginnen Nederlands eerste kritische computerblad.

Hack Tic is een nieuw maandblad voor hackers. Het bevat alle trucs en tips die andere bladen niet hebben. Maakt over Computer-Hacking, Phone-Hacking of andere vormen van technica-avontuur vindt je altijd eerst in Hack Tic.

Maar ook achtergrondverhalen over informatisering(schandalen), grote computer-netwerken en de onvermijde opslag van privacy gevoelige gegevens komen aan bod. Zoekende is Hack-Tic interessant voor iedereen die zich kritisch opstelt ten opzichte van de informatiematschappij.

Hij, Brother

Want Hij, Brother lijkt steeds vaker mee, al doet hij dat in onschuldig lijken de vermoedelingen. Het gerucht doet de ronde dat hij zich in Nederland heeft vermomd als groomsman. Ook zou hij de man achter de schermen zijn bij het rood pin ring plan van minister Smit-Kroes. Vast is hij echter anders overtuigd. Op zijn orders worden in Nederland steeds meer databanken gekoppeld, om iets moet wel een nog goed bewaard geheim zijn als het niet met een druk op de knop door elke ambtenaar is op te vragen. Hack Tic zal regelmatig berichten over nieuwe vermoedelingen en plannen, en je door middel van 'in depth' reportages zijzelf op de hoogte houden van de laatste ontwikkelingen.

De informatiematschappij wordt geregeerd door een klein clubje machtige heren op werkdagen, die van ver af de hoogte doorgeven wat goed voor ons is. Zij bepalen namens het grote bedrijfsleven welke systemen er worden ingevoerd, zij bepalen welke gebouwen er wel en niet van de computer gemaakt worden. De buitenstaander wordt niet geacht mee te denken. Maar dan mag hij wel: "Koop maar een PC en een tekstver-

werker en ga maar oefenen, aan typen en typen is nog behoefte genoeg. Als je braaf je best doet mag je volgende week gegevens intypen in een database."

Banities is het maar

Hackers willen een geïntegreerde maatschappij waarin mensen zelf kunnen beslissen welke informatie ze tot zich nemen. Een maatschappij zonder computer misstaat. Maar als hackers in het algeen leven staan steeds de techniek voorop. Hackers moeten rechtspalen en het technische wonderland opzien. Kritische opmerkingen worden zo mogelijk weggevoerd achter het technische bril van de hacker, en anders de storm van gaan liggen waan de zaken even zo als ze waren een door onbemande geregeerde valleiacht waar niemand meer wijt uit wordt, hoogaat om beter beveiligd tegen 'ontveegde muziek'.

Het werd dus tijd voor een eigen hacker gelid.

Hackers staan per definitie kritisch te genover de informatiematschappij, al is het maar omdat die kritisch tegenover hen staat. Hackers komen echter nog te vaak over als strijders voor goede computerbeveiligingen. Ze worden maar al te vaak misbruikt als schutkleed voor bedrijven die systeembeveiliging aanbieden. Het is niet het doel van de hackgemeenschap om beter beveiligde computers te krijgen. We zien liever dat er goed gebruik wordt gemaakt van de techniek. Systemen die de privacy van mensen niet beter beveiligd, ze horen niet te bestaan.

Nieuwe mogelijkheden

Het kan andere computers kunnen worden gebruikt om mensen snel van informatie te voorzien. Ze kunnen grote

groepje mensen uit de hele wereld samen deelnemen in computer conferenties om te komen te weten van de nieuwste stand van zaken. Informatie over rampen kan sneller bekend worden, regeringen van waterschappers kunnen sneller worden ingelicht. Mensen uit de hele wereld kunnen goedkoop en snel met elkaar corresponderen. Computernetwerken kunnen de menselijke samenleving waaruit helpen.

Wat al deze prachtige mogelijkheden hoort je nu nog niets. Misschien geloof je er niet eens in. In onze artikelen zal regelmatig besproken worden hoe je met computernetwerken om moet gaan en hoe je zonder al te veel geld te besteden kunt beschikken over de informatie die je wilt hebben.

Wereldwijde

Hacken is internationaal. Grote databanken, informatiemonopolen en bestaande koppeling zijn dat ook. De wereld komt dichterbij elkaar en de tijd dat hackers al leur internationaal niet nodig hadden is voorbij. Zie jij je al lopen in het Europa van 1992, met een suitcase op zak en een identificatiekaart onder je arm? Gelukkig staan we niet alleen ook in het buitenland zijn hackers actief. Met al deze organisaties (zoals de Chaos Computer Club in Hamburg) zal internetsel worden samengewerkt zodat ook in 'Vier neue Europa' altijd een hack geluid te horen zal zijn.

Het belangrijkste komt er in dit stukje bekend al. Naar HACK INFORMATIE, daar zal Hack-Tic vol mee staan. Mensen met een technische interesse kunnen hun hart ophalen aan de vele technische knutsels en tips. Alles voor de computerfreaken en de infoconnuistiek. Soms vastlagen van complete hacks met alle technische achtergrondinformatie, soms hacks voor nog te plagen hackers. Hack-Tic stelt zich tot doel om alle ontwikkelingen op hackgebied in haar ko-

lonnen te hebben. Ook als de technische details je niet duidelijk zijn wil je in elk artikel de omgeving en betekenis van een hack kunnen lezen. We hebben geen geheimen, informatie is vrij!

Als je dit blad de moeite waard vindt kun je iets terug doen omk jezelf abboneren. Den je dat al, vertel het dan je vrienden/verliefden. We geven dit blad niet uit om er zijn van te worden en voorlopig maken we er alleen maar verlies op. De prijs van Hack-Tic is laag omdat we hopen dat veel mensen behoefte hebben aan onze informatie. Tenzij dat niet en maak 35 gulden over op bankrekening 94.72.84.541 en je krijgt 10 nummers lang het grootste, dikste, voordigste, leukstijfste en enige hackertijdschrift van de Duitse in de bus.

'Hacking is a way of life' zeggen verre voorouders al in de jaren veertig. Natuurlijk gaat Hack-Tic ook mee in de wereld van de hacker, een wonderlijke, open wereld vol eigen humor. Hacken is in ieder geval een kunstvorm die zeker niet is voorbehouden aan mensen die cranial met een computer om kunnen gaan. Ook op andere technische gebieden zijn hackers actief, en als je definities longen haartwist is iedereen die zich verset tegen de gevestigde orde, bestaande middelen cranial gebruikt en zich niet stoort aan regels, een hacker.

Een tijdschrift beginnen heeft veel overblikken met een gekochte Zelf in onze wereld vol computers en techniek is het nog maar de vraag of de baby te vervuilen is. Al is deze baby nog niet zo nieuw, met haar grote mond denkt ze het nodige gewicht in de schaal te kunnen leggen.

PROOST

De Redactie

kopij gezocht

We waarderen redactionele bijdragen. Klachten over automatisering op de zaak? Schrijf een informatie over nieuwe databanken? Schrijf een kluswerkstuk om leuke dingen te doen met de telefoon? Schrijf een Complete hack gepieegd? Schrijf een (en vergeet niet je logfiles mee te sturen). Het hoefden geen hele artikelen te zijn, ook tips zijn soms goud waard. Natuurlijk, hoefden we je naam niet te weten; What's in a name anyway?

Stuur je informatie naar:

Hack Tix
Postbus 22953
1100 DL Amsterdam

telefax 020-763706
tele 12949 gratis al
smap _freewaresoftware_
foto 2-2001 Hack Tix



As safe as the Bank of England?

Electronisch kluisensysteem diefstalgevoelig

Een geheel elektronisch kluisensysteem is sinds enige tijd operationeel op het Amsterdamse Centraal Station. Dit systeem waakt dagelijks over de toegang van honderden reizigers. Er blijken echter de nodige frakke te zijn om dit systeem op te lichten. De mensen achter dit systeem blijken net zo betrouwbaar als hun apparatuur: ze weten dat er iets mis is, maar houden tegenvoer de nodiger wel dat het zijn eigen schuld is.

Een reportage van Herman Acker

Het lijkt zo handig: je stopt je bagage in een kluis en doet de deur dicht. Vervolgens koop je naar de tijd jouw ticket (horende betaaltreinstand en betaalt fl. 1,50 fl. 3,- voor de grotte kluisen). Het apparaat print dan vervolgens een bar code kaartje (op een printerje uit het jaar met maakt een tikbelletje en doet er oeven over).

Met dit kaartje kun je het kluisje dan binnen 24 uur weer openen. Een je te lost dan moet een boom worden betaald. Het kaartje werkt (zoals in het Nederland is uitgegeven op de kluisen) maar 1 keer. In de kluisen gepieegd dan staat het apparaat een kaartje in de linker onderhoek van je kaartje om van te geven dat de kaartje al eens is gebruikt.

De tijd op het station rondhangende reizigers van bagage en kluisen heeft echter al een aantal methoden

betreftheid om de gebruikers van dit systeem van al die nieuw koffers te voorzien.

Trank 1: Ik duw mijn kluis dicht en loop naar de terminal om te betalen. Een andere man staat daar voor zijn kluis te betalen (steek ik), dus ik wacht geduldig op mijn beurt. Als de man klaar is duwt een medeplichtige met zijn voet een ander kluisje in hetzelfde blok dicht. Ben ik aan de beurt dan betaal ik voor dit kluisje lang dat. Het als ik terug kom en het lege kluisje openmaak zie ik dat het kluisnummer op mijn kaartje niet klopt. Maar dan is het al te laat.....

Trank 2: Een stel Amerikaanse Amerikanen staan te bemoeien met hun bagage. "Nice city, Copenhagen". "Shut up John, this is Amsterdam, give me that suitcase. Oh these stupid computers."

Op het toppunt van hun gehoorzaamheid een goed Engels sprekende heer zijn diensten aan. Hij weet wel hoe het systeem werkt. Je sluit je spullen er in en betaalt. Je krijgt dan een kaartje en dat kun je nu vaak gebruiken als je wilt om weer in je kluis te komen. Nu ja nu is het niet geldig. Hij raadt je wel aan om het even te testen, want zeker weet je het niet door dingen nooit.

De vertroouwende Amerikanen gaan haast huilen van zoveel behulpzaamheid, stoppen snel hun spullen in de kluis en betalen voor de kaart. Daarna proberen ze hem nog even uit. Gewarptheid dat alles in orde is steken ze hun kaart in de sok, duwen de kluis dicht en lopen weg.

De computer instructies denkt een stel nieuwe klanten te pakken te krijgen en wil weer geld zien. Als binnen anderhalf uur minimaal niet betaald wordt, opent het apparaat hoor de kluis in bewaart en gaat weer digitale schuifjes toeren.

Trank 3: Simpelere variant op trank 1. Je duwt stuk voordat het slachtoffer zijn kluisje dichtdoet een ander kluisje dicht en kun het slachtoffer voor dat kluisje be-

halen. Nadat hij klaar is wacht het systeem anderhalve minuut en dan... klik!

Toen ik de geruchten over dit nieuwe systeem hoorde heb ik de proef maar eens op de man genomen. Ik heb een lege kluis geboden en een later die nacht teruggekomen om hem weer te openen. Ik deed alsof ik het slachtoffer was van trank 1. "Help, ik stap mijn kaartje er in en het ding doet de verkeerde kluis open." Ik belandde via de bagagevervoer van de NS ("Oja, dat is natuurlijk Uw eigen schuld. Nouja, daarvoor zijn wij niet aansprakelijk") uiteindelijk bij de spoorwaggon. De daarbijkomende agent vertelde mij een aantal interessante details, waaronder de bovengenoemde trank, maar hij vertelde me:

"De NS is het gekke met de kluisen nu. Alle informatie over onregelmatigheden met de kluisen die wij hier inzoomen gaat naar de juridische afdeling van de NS. Die kunnen dat weer gebruiken voor een juridische procedure tegen de exploitant."

De juridische afdeling van de NS spreekt hij mondt van Ditz. Doordat veel van een juridische procedure tegen de Rijk (Bagagekluisen Exploitant Maatschappij). Maar dat die het met de Amsterdamsche vervoerkluisen te maken heeft is Uw eigen conclusie. In het belang van de NS en Service kan ik over de proef daar niet zeggen." (Service is een volle NS-dochter die onder meer de afgifte van exploitatievergunningen voor staatskluisen regelt.)

In de Rijk zelf? De in Roermond gevestigde firma laat haar telefoonlijn door een antwoordsysteem openstaan maar vergoet het beldje al te laat.



SPORWEGSPOLITIE
STATIONSPOLITIE
1100-1101

"Gedrukt door de Staat."

Land (P) van de Staat
Datum: 8
Jahr: 1988

Naam: Wouter van der

Adres: Wouter van der

Tel nr: 1100 1101

Naam, adres en telefoonnummer van de afzender

Naam afzender

Wouter van der

Land (P) van de Staat

Wouter van der

Naam

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

De afzender is gesigneerd

Wouter van der

Land (P) van de Staat

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

Wouter van der

OPLEIDING TOT TELECOMMUNIST

deel 1

In Amerika begon het al in de jaren zestig. Het door Bell (Amerikaanse PTT) uitgelegde telefoonnet kon door middel van een toonstelsysteem om de hele wereld geleid. Er ontstond een subcultuur van 'phone phreaks' (jongen die t's door de pb van 'phone' vervangen). Nu 'Ma Bell' veel centrale's vervangen heeft door onkraakbare types en op allerlei andere vormen van creatief telefoongebruik zware straffen heeft gezet is de cultuur aldaar een beetje aan het uitsterven. Hier in Europa, waar alles later komt, is phreaking nog een redelijk nieuw gegeven.

Door The Rip en Peter Aalhuizen

Het internationale telefoonnet lijkt misschien een tamelijk gesloten systeem. Maar als je wat vaker internationaal belt zul je gemerkt hebben dat aan het begin en eind van een internationaal gesprek vaak de vreemde papjes zitten.

Deze papjes zijn de controlebladen die heen en weer op de lijn gaan. Ze vertellen de centrale van ontvangende land met wie de belter contact wil en de op belkende centrale krijgt via het zelfde systeem van papjes informatie over de voortgang van de gespreksopbouw. Als bijvoorbeeld de opbelder neerligt en dus bekend is dat langer prijz zit op de verbinding wordt door middel van een papje aangegeven dat de lijn weer vrij is.

Een ding ligt het zwakke punt van dit type 'signalerings'te te spelen zich geheel af buiten de netwerkbund. Dit wil zeggen dat alle gebruikte papjes ook over de gewone 'customer' lijn getransporteerd kunnen worden. Als ik een nummer in land X bel en dan het 'denkige is weer vrij papje' op de lijn het geeft mij contact dat gewoon door aan de 00 centrale. Deze het alleen op papjes van de andere land en geeft het papje ook gewoon door. De ontvangende centrale in land X stuurt echter contactlijst met het opheffen van het aangevraagde gesprek. Met een serie van nieuwe papjes kan de centrale dan gevraagd worden een nieuwe verbinding op te bouwen (ook met nummers buiten land X).

Natuurlijk zijn de PTT's zich bewust van dit probleem, en nieuwe internationale lijnen reguleren dus ook met meer dan een de sprekbund, maar op frequenties die op gewone telefoonlijnen niet worden doorgegeven of door een nog nieuw systeem met een gemeenschappelijk kanaal waarop alle signalering plaatsvindt.

De oude systemen zijn echter nog aanwezig in gebruik om garant te staan voor een van juist en plezier. In dit artikel zullen we uitgebreid ingaan op het signaleringsysteem CCITT 4. Dit systeem is vooral op oude lijnen in Europa nog uitgebreid in gebruik. Het is bekend ge worden tijdens de 'Denemarken affaire', waarbij het bleek dat een GRATIS 06 nummer gevonden dat doorzieldde naar een bedrijf in Denemarken. Zodoende kon men dus voor niets met de hele wereld bellen.

Het systeem werkt met toonreeksen, in principe opgebouwd uit 7 elementen.

Elementen

F	150 ms 2040-2400 Hz
X	100 ms 2040 Hz
Y	100 ms 2400 Hz

XX	350 ms 2040 Hz
YY	350 ms 2400 Hz
X	35 ms van 2040 Hz
Y	35 ms van 2400 Hz

Toetsreeksen

Van belzonde naar ontvangende centrale

Terminal seizure	PX
Transfer seizure	PY
Clear forward	PXX
Forward transfer	PYY
Cijfer 1	yyxx
Cijfer 2	yyxy
Cijfer 3	yyxx
Cijfer 4	yyxy
Cijfer 5	yyxy
Cijfer 6	yyxy
Cijfer 7	yyxx
Cijfer 8	yyxy
Cijfer 9	yyxy
Cijfer 0	yyxy
Call operator code 11	xyxx
Call operator code 12	xyyy
Spaak	xyxx
Incomung echo sup.	xyxy
ST end of-paging	xxxx
Spaak	YYY

Van ontvangende naar belzonde centrale

Trans. proc./to-send	X
Transfer proc. to-send	Y
Number received	P
Busy flash	PX
Answer	PY
Release guard	PYY
Blocking	PX
Unblocking	PYY

Gebruik

Deze tabelken zijn natuurlijk geschikt om te zien, maar wel doe je er mee. Alvorens moet je een methode hebben om deze tekenjes te genereren. Hiervoor kan je een halbbrecomputer gebruiken mits die

in staat is om twee tonen tegelijk te maken (dus geen IBM PC of klomp).

Ben je zover, dan is de rest simpel: je maakt eerst een gesprek dat via een CCITT 4 (C4 is korter) lijn loopt. Als je genoeg ervaring met deze methode hebt kan je dat horen als een gesprek tot stand komt, maar voorlopig zal je het moeten hebben van erg veel proberen (misschien brengen we over een tijdje wel een cursus-cassette op de markt...)

Heb je eenmaal zo'n lijn gevonden (ga die, dat wel tegen een lagere prijs dan wat je eigenlijk voor het gevonden je spreekt zoo gaan betalen), dan geef je het 'Clear forward' signaal. Dit laatste om te zeggen, dat je zelf moeten weten meten om het juiste moment te vinden (bijvoorbeeld na het tweede klikje op de lijn).

Op bepaalde lijnen hebben ze een grap je uitgehaald om dit eenvoudig te maken, in dat geval is de lijn na het geven van het 'Clear forward' signaal onmiddellijk in gesprek. Dan heb je pech gehad en zal je een andere lijn moeten proberen.

Als alles goed gaat hoor je een het 'Clear back' signaal. De andere kant heeft door middel van dit signaal beseft dat de lijn vrij is en is opgehoorden met het tot stand brengen van het overprontelijk aan gezonde gesprek.

Je kunt nu twee dingen doen: je kunt een gesprek beginnen met een abonnee in het land waar ook de zijde 'afgeplaat' centrale staat, of met een ander land. In het eerste geval kun je de centrale als directieken en geef je het 'Terminal seizure' signaal. Wil je naar een ander land bellen dan geef je 'Transfer seizure'.

Na 'Transfer seizure' komt de centrale met een Transfer proceed to-send. Nu kan je de landcode intekenen met behulp van de cijfer toetsen van de lijn. Na het intekenen van een cijfer geeft de centrale korte toetsjes terug. Een 'Y' betekent dat er nog meer cijfers nodig

Zijn, een 'x' (iets lichter) wil zeggen dat er geen ergers cijfers binnen zijn. Na het laatste cijfer even wachten. De volgende centrale is de keizer komt dan of met een 'Terminal proceed to send' of met nog een 'transit proceed to send'. In het laatste geval moet je nog een keer het landnummer inspreken, net zo lang tot je bij een centrale in dat land aankomt.

Nadat je een 'Terminal proceed to send' hebt ontvangen moet je eerst het gesprekstype aangeven (bijv. 'direct dialing digit'). Hiervoor kun je gewoon een nul nemen (anders digite zijn voor operatieposities v.d.). Daarna komt het 'national significant number'. Dat is het telefoonnummer van de abonnee die je wilt spreken, zonder de eerste nul. Nu even wachten op verbinding en klaar is 'De koningstijd'.

Voor de gevorderden is deze truc niet alleen bruikbaar om tegen goede oord te bellen. Zij kunnen zich voordoen als operator en zo allerlei leuke gesprekken opbouwen, zelfs met landen die totaal niet automatisch bereikbaar zijn (zo neem je de overbetachte PTT mede-werkers wat werk uit handen, laten we het zijn voor elkaar).

Ook moet nog gezegd worden dat experimenten met deze methode gratis is: de kosten gaan paar kopjes op het ma-munt dat er een verbinding tot stand komt (dus als er een de andere kant is maar opbrengt). Je betaalt altijd de kosten voor het comprimerende gekozen nummer, ongeacht waar het gesprek uitmondig uitkomt. Dit betekent dat als ik een 06-0 nummer heb dat doorkomt over een C4 lijn, ik dan helemaal niks betaal, omdat mijn centrale denkt dat ik met een gratis nummer aan het bellen ben.



THIS, The Hacker Information System

*020 - 717000
(020) 1200, 1200, 1200, 1200-700*

In een ver verleden waren er in Nederland maar een paar hackers. Na het eerste hacke de krachtoppen hadden gebald werden het er echter spoedig meer, en al gauw werd het hackerswereldje een tikje chaotisch. Het werd tijd voor een kleine beetje ordening in de warige telefonische gesprekken en berichtenuitwisseling. Het idee voor THIS (The Hacker Information System) was geboren, een specifiek hacker BBS.

Er werd begonnen met THIS op een PC engine in Rotterdam. Er was toen maar 1 telefoonlijn en 1 PC. Het BBS was echter drukbezet. Te drukbezet de telefoon stond niet stil en het BBS was onbereikbaar. Toemidsg toeop Cries Tijdig zocht contact met Max Kiezer, sysop van NEARBS, ook toen al Nederland grootste bulletin board, over de mogelijkheid om THIS onder te brengen als een sub board in NEARBS.

BEL GRATIS

Het idee was dat beide partijen daarmee beter af zouden zijn: THES krijgt betere faciliteiten (na: 16 lijnen, telex, fax en UUCP en foto netwerk) en NEABBS krijgt extra klanten.

Want leers of begintmen uit andere hobby's: het is NEABBS uitgegroeit tot een volwassen bedrijf in BBS telecommunicatie. En hoewel bereikbaarheid is ook knaster voor de vele synops die hun BBS van een zonder daarvoor geld van hun gebruikers te vragen, is het wel of er gratis BBS'en zijn die hun gebruikers hun een bieden wat NEABBS heeft. Dit alles betekent echter wel dat je voor de toegang tot NEABBS moet betalen 6 cent per minuut. Dit doe je door een zelf voor te stellen betaling over te maken naar NEABBS.

Elke maand dat je NEABBS gebruikt loopt je krediet dan af met 6 cent. Naar je de rode cijfers dan staat NEABBS je een herinneringsbericht zodat je nieuw geld kunt overmaken. Als je gebruik maakt van de speciale faciliteiten van NEABBS (telex, telex, versafontoproepen, UUCP samen, FIDO Echo's etc.) wordt extra geld van je krediet afgetrokken.

Ik kan me goed voorstellen dat je denkt: "Tja knaster omre ik betaal genoeg voor mijn hobby; de computer is duur en de PTT is veel te duur. En dan zeker ook nog eens voor een BBS gaan betalen is niet wel uit". Het enige alternatief is echter een gratis BBS met voldoende minder faciliteiten en minder betrouwbaarheid, zodat het lang niet altijd toegankelijk is.

Verder over THES; terwijl het aantal filies gestaag groeit, heeft THES te maken met duidelijk op en down in de bereikbaarheid. De ene maand sterft het er van de bereikbaarheid en tijt het wel about er in de hele wereld geen enkele computer staat, de volgende maand worden er maar twee of drie bereikbaar gepost.

Insidelen zijn Peter Hekkers en ondergetekende en synops (schippers naar God) van Nederlandse grootte hacker BBS, met enkele magabytes van informatie over de meest uiteenlopende onderwerpen. Het beleid van THES (net als we het alstet alstet hebben met andere dingen ontbrekt het nog wel een een beleid), is het er op gericht om THES voortdurend te houden en te proberen alstet over een gevarieerd aanbod in nieuwste en laatste te worden.

Een van de grote dilemma's in THES is alstet Hoeveel informatie geven we de beginner? Het is natuurlijk heel simpel om de groep 'juwonderde' hackers alstet informatie bereikbaar te stellen, maar het is een beetje naar als je met een groei van een hack bezig bent en een goedbedoerde beginner maakt in zijn onwetendheid de systeembeheerder alstet op de hack. Gevolg: weg hack.

Daarom is THES verdeeld in twee's. Nieuwe gebruikers van THES komen na het aanvragen van toegang binnen op level B. Hier kunnen ze alleen maar de openbare bereikbaarheid lezen en nog foto maar geen foto downloaden. Zodra er een bijdrage aan THES is geleverd (niet noodwendig hack kennis, wel hack betrouwbaarheid) wordt de gebruiker 'upgraded' naar level C.

Level D is voor de hacker die heeft in een idee wat hij kan' en level E is voor de voor een kleine groep van ingewijden. De oplopende level betekent hier dat je vel E magbruikt is, maar het is alstet hoe dig om een level over te hebben.

Het is natuurlijk omre om alstet in te vele in te delen, en als voorbeelden van de 'flow flow of information' vind ik dan ook dat alle informatie die geen betrekking heeft op nog in gang zijnde hacks afg moet zijn voor iedereen die een van THES bijdrage.

[RCP]

In deze rubriek korte stukje informatie, of juist vragen om informatie. Antwoorden naar de redactie postbus, telex, fax etc. etc. Nu staan hier een aantal vragen die ons zo veel te benaren schieten, de volgende keer zijn jullie aan de beurt.

Hacken onder Hoogspanning

Op het elektrotechnisch vlak lang niet alleen spanning die nodig is om allerlei hardste apparaten zoals mijn computer te laten draaien. Via het net worden ook de nodige stroomsignalen op de lijn geprojecteerd. Een signaal met een veel hogere frequentie maar een kleinere amplitude wordt gebruikt om bepaalde zaken aan te duiden.

Ik woon zelf in de Zaanstreek en ik heb laatst een elektricien over de vloer die mij van alles wist te vertellen over dit systeem. Zo zijn er kuren die straatverlichting aan en uit schakelen. Maar ook de dag- en nachtelijke voor de industrie ('s nachts is stroom goedkoper) worden nu op deze manier bediend.

Ik rasp natuurlijk onmiddellijk: "Je maar, als ik zelf die toren nou eens op het net zet vanaf het eerste het beste stopcontact?" Daar had de goede man geen antwoord op, maar de stilte die volgde speek troostelen.

Ikzelf heb helaas niet de nodige apparatuur en kennis om een en ander uit te zoeken. Wie maakt een apparaatje dat een nu of het nacht-puls uitstraalt zodra de radio het dag-puls is ontvangen?

Peter Poelman, Krommenie

Tele-Gambling

Enger is Delft staat een leuk ding aan de telefoon. Je belt het en dan neemt het op met een pieptoon. Nu kun je verscheidene vijf cijfers intikken (op je DTMF toefoon), waarop een serie stellingpiepjes volgt (juist de code niet goed is).

Waarschijnlijk kun je allerlei leuke dingen doen als je de goede code weet, maar ja. Iedere poging kost vijfteen cent, dus als je na 50000 keer proberen kort hebt heeft dat jou (of je baas...) 1.7500 gekost (pijng, kass).

Wat leukste kortje nog als je dit meer mer indikt op de DSB computer zeg het heb (draait onder VMS, vandaar) dat op dat nummer geen aansluiting zit. Waar moet het heen met de wereld als je niet meer op de PTT computer kort verhoort wen voor je informatie...

Hier is de 045-763900, wie de code vindt krijgt een appeltaart.

John D. & The Key

Door schakelen wijs

De PTT levert doorschakelapparaten. Deze stannen nog uit de tijd dat doorschakelen niet in de centrale maar nog ge-woon bij de abonnee thuis werd gedaan (op wat oude centrale's is dit nog steeds zo). Het nadeel is wel dat je twee tele-lijnenlijnen nodig hebt.

Wel je op de volgende lijn van dit apparaat dan kun je met een speciaal pieperijje ontdekken waar het ding naar doorschakelt. De toontjes die door dit pieperijje ge-maakt worden zijn geen DTMF toontjes, maar een soort riedeltjes.

Wie weet meer?

Eddie, your neighbourhood hacker

Wij zijn niet bang voor de tandarts.

Colgate mag dus, als we de reclame geloven, beschermen tegen gaatjes, maar de gaatjes in het wereldwijde computernetwerk van Colgate/Palmolive liegen er alid om.

Ik hoor echter al systeembeheerders zeggen dat hun systemen wel veilig is. Ik kan u verzekeren dat er geen veilig computers bestaan en dat ze waarschijnlijk ook nooit zullen bestaan. Mocht er echter ooit een 100% veilig computer komen dan is er nog steeds de menselijke schakel, die zoals we anders hier weer merken, de zwakste schakel is in de beveiliging van een computer.

Het computernetwerk van Colgate/Palmolive bestaat voor het overgrote deel uit computers van het merk Digital, type Vax, waarop is de geval het VMS operating systeem draait. De computers waren met elkaar verbonden door... het zogenaamde Decnet. Dit netwerk maakt het mogelijk om over de hele wereld te werken, gegevens en post te verspreiden. Zo was het dus mogelijk om vanuit Luik (België) post te versturen naar bijvoorbeeld de vestiging in New York. Ook was het mogelijk om bijvoorbeeld als gebruiker van de vax in Luik, gebruik te maken van de vax in New York (waar misschien software en informatie is die voor bepaalde gebruikers over de hele wereld van belang kan zijn). Zo was het voor ons (een vriend die ook lezer van deze tijdschrift is ik) heel makkelijk om van de ene computer over te springen naar de andere, zodat we op een gegeven moment bijna over de hele wereld heen konden lopen in vergaderingen van Colgate/Palmolive.

Het werd een absurde om vanuit zijn woonplaats door te schakelen van België en Italië naar bijvoorbeeld Amerika, waar op dat moment computers die misschien wel kunnen kraken, bezig zijn om jouw data te verwerken. Het is nog leuker om te weten dat je evenwel privileges hebt als de eigenaar van de computer. Het enige wat hij meer kan, is de stude ruitjes uit het stopcontact trekken, wat hij niet zal doen zolang hij niets van jouw aanwezigheid heeft gemerkt. Doet hij het wel dan is hij nog welken, misschien wel maanden bezig om zijn systeem "opnieuw" te beveiligen. Daarbij denk ik dan aan een operator die hij zijn basen op het netje wordt genoemd en gevraagd wordt of het systeem "weer" veilig is, waarbij de operator (skatend aan vrouw, kinderen en de komende zomer op Mallorca) alleen maar positief kan antwoorden, terwijl hij zijn hart verhoudt bij het weer koppelen van zijn systeem aan de buitenwereld (om te horen, dat niet).

Toegang tot

Doormiddel van het langzaam ophooven van de privileges kregen wij o.a. toegang tot project en financiële gegevens. Het was voor een groot bedrijf natuurlijk fatal kan zijn. Tevens konden we de post en teled berichten (dus liegen ook via de computer) van anderen lezen, beichten over beredding en verkoop van de produktie lepen dan over ons schem. Nog interessanter waren de beschikking van operators aan elkaar, zij vroegen elkaar om toegang op elkaars systeem, waarna er gelijk een bericht ingehouden met de login, het password en de mededeling dat de goedgekeurde FULL-PRIVS kreeg op het systeem, waarna wij dan weer volledig toegang kregen tot een andere computer in het Colgate-netwerk. Zo drongen wij binnen in een

groot aantal computers van het Colgate concern.

De techniek.

Vaak hebben wij op de van in België (RND/C) een klein gekregen, zoals dat altijd gaat, een klein met lage privileges, maar goed genoeg voor ons doel, want het enige wat wij nodig hebben is de gebruikerslijst en de nodulen. Nadat wij daar waar ons toe gekund hadden zagen wij dat de gebruikerslijst een groot aantal potentieel bruikbaar logins bevatte, en wonder boven wonder vond Colgate het ook nodig om zelfs een van deze logins full price te geven.

Nadat wij erachter van deze stormse had bijwonen, en we ingelichten de systeembeheerder hetzelfde bevelen voer volgden wij onze weg in het systeem. Dit ervaring was gebieden dat als we geen bewijs zouden hebben, Colgate ons nooit zou geloven als we dit vertellen, dus bevelen we ons eerst, en uit elke rode een logins te gaan bijhouden (zoals fragmenten bijvoegde).

We ontdekten zelfs met AUTORIZIE (een programma wat normaal alleen door de systeembeheerder mag worden opgestart) dat de systeembeheerder zelf zijn password al ongeveer een jaar niet heeft veranderd, wat natuurlijk ook je niet begrijpen nog riken is. Maar oh, dat is nog niets vergeleken met de andere fouten in het systeem.

Zo bleek het dus mogelijk om de verschillende files zoals de userlist en node list via de computer in België van verschillende computers over de hele wereld af te halen zonder dat wij daar een login hadden. Op deze manier vergaarden wij dus informatie over gebruikers van systemen, over de available internetinfo en over de network mogelijkheden. Dit was dus gewoonweg niet mogelijk, want in principe staat er valt je toegang tot de computer, en op deze manier is het voor

de concurrent heel simpel om de eventuele concurrentie van Colgate te prieten. Nog erger was het dus als er in dit geval veel persoonlijke gegevens zouden uitbreken, die in dit geval beperkt bleven tot de gegevens van gebruikers en dat soort dingen. Toch is het een heel klein stuk want we weten wat er met uw informatie gebeurt in het bedrijf waar u werkt. Hoe wordt uw informatie ingehouden?

Ik wil echter nog een ding zeggen tegen systeembeheerders, denk nooit dat uw systeem veilig is want misschien komt u volgende maand een artikel over uw systeem. "Never say never again".

Jefrey C. (1989) weet veel beter!

[In de door de heer C. ingezonden stapel print ook het volgende]

Een index.....

September 15, 1988

subject: port competitive activity

for your information, please note that the uk company has identified a market or search placement test of xoxo liquid in a 1 liter, handled bottle.

product description/az - 1 liter deliverable cream

contents/needs include:

"recommended by leading three main manufacturers like xoxo and yyy"

"xoxo is recommended for deliverable machines, including however, tested, and tested"

i bring this to your attention for the obvious reason of increased competitive activity within the region. further demonstrated by xoxo's recent expansion of xoxo liquid add in netherlands. perhaps more of note is the focus and ability of yyy to secure such a wide range of manufacturers' endorsements -- an area we should continue to actively pursue.

please keep me advised of any/all competitive developments in your market in

they relate to add's and, in turn, I will insure all operating units with a vested interest are kept informed.

regards, Harry Blackell

[Omdat we weten dat Colgate/Palm-Bee before advocate heeft die wij hebben we alle namen, kinderen etc. veranderd]

Even submenus.....

502 FRINGE BENEFITS

5020 HOURS

5020 VACATION

5020 PAYROLL TAXES

5020 PENSION PLAN

5020 LIABILITY & GROUP

INSURANCE

5020 LEAVING INDEMNITIES

5020 HOSPITALISATION

INSURANCE

5020 TRANSPORT INDEMNITIES

5020 OTHER FRINGE BENEFITS

(icht-verl...)

Can selectie uit de aangesloten systemen.

reache Colgate

Natuurlijk is ook Colgate opgebeld voor een reactie, en die was vóórgepoetst: "Ik heb het niet gedaan, daarvoor is XXX verantwoordelijk."

Na 3 uur belten met ditmaal het stels in Nederland en België waren we 25 gulden armer en nog geen cent verder. De automatische ringel-acht voor de Deurema heeft volgens eigen zeggen met het FAX-netwerk niets van doen (dit is al een hele veronderstelling de rest van de automatiseringen mochten we niet afleggen en wat was het bij).

	Node	Link	Cost	Hops	Next Hop to Node
1.12	RNDLG	0	0	0	(Local) - 1.12 RNDLG
1.1	PARKAY	0	4	1	INT 0 - 1.1 PARKAY
1.2	DCVAX1	0	4	1	INT 0 - 1.2 DCVAX1
1.4	TCOF	0	4	1	INT 0 - 1.4 TCOF
1.5	BADGE	0	4	1	INT 0 - 1.5 BADGE
1.6	PSNAG1	0	4	1	INT 0 - 1.6 PSNAG1
1.7	ARTHUR	0	4	1	INT 0 - 1.7 ARTHUR
1.8	RCSNA1	0	4	1	INT 0 - 1.8 RCSNA1
1.10	TCVAX1	0	4	1	INT 0 - 1.10 TCVAX1
1.12	RNDRC3	0	4	1	INT 0 - 1.12 TCVAX2

WORM OP HET INTERNET

Het internet verbindt een groot aantal research computers in de hele wereld. Een waarneming sluitende programmeur heeft een programma ontwikkeld dat zichzelf reproduceert en zeer efficiënt over het netwerk kan verspreiden.

Op het internet wordt ook nieuws over diverse onderwerpen over de aarde gedeeld. De nieuwsgroep "USENET" (The data of computing) bevatte vorig jaar november een groot aantal interessante berichten. (De hele structuur van de website was al bekend toen de pers hier nog schreef dat "men in het donker leeft". Nu nog heeft de pers het over een virus in plaats van een worm. De artikelen spreken voor zich...

De Gang

It's now 3:45 AM on Wednesday 3 November 1988. I'm tired, so don't bother me everything that follows...

Apparently, there is a massive attack on Unix systems going on right now.

I have spoken to system managers at several computers, on both the east & west coast, and I suspect that may be a system wide problem.

Symptoms: hundreds or thousands of jobs start running on a Unix system taking response to zero.

Systems attacked: Unix systems, 4.3BSD and its variants (eg. SUNs) any sendmail compiled with debug has the problem. See below.

This virus is spreading very quickly over the Milnet. Within the past 4 hours, I have evidence that it has hit 10 sites across the country, both Argonne and Milnet sites. I suspect that well over 50 sites have been hit. Most of these are "major" sites and gateways.

The bug in Sendmail

When the Unix 4.3 BSD version of Sendmail is compiled with the Debug option, there's a hole in it.

Most Unix systems (BSD 4.3 and Sun) apparently do not have this bug. It exists only where the system manager re-compiled Sendmail and enabled debugging.

That is bad news.

Date: Thu, 03 Nov 88 22:04:15 EST
Subject: A cure!!!

FLAME!!

Kevin ("Ain't your friend?") Evans don't just burst into my office with a cure discovered in the disassembled worm to my.

If there is an external variable in the library named "plousquel" that is not zero, the worm will die immediately after eating. Thus, to kill any new worms, include a patch in your library that defines the symbol. The following shell file and source code will modify your C library to define this symbol.

It WON'T kill any currently linked and running versions, but it will prevent reinfection.

Subject: The Worm

Our site apparently didn't get hit, because our newly installed NFSnet server has been so flaky that it has been unusable. Just goes to show, I guess.

A REPORT ON THE INTERNET WORM

Bob Page

University of Lowell
Computer Science Department
November 7, 1988

Here's the scoop on the "Internet Worm". Actually it's not a virus - a virus

is a piece of code that adds itself to other programs, including operating systems. It cannot run independently, but rather requires that its "host" program be run to activate it. As such, it has a clear analog to biologic viruses — these viruses are not considered live, but they invade host cells and take them over, making them produce new viruses.

A worm is a program that can run by itself and can propagate a fully working version of itself to other machines. As such, what was loose on the Internet was clearly a worm.

The basic object of the worm is to get a shell on another machine so it can re-produce further. There are three ways it attacks: *smfmind*, *fingerd*, and *rtshrewc*.

[*then volgt langdradige technische uitleg*. Het komt er op neer dat de worm probeert om via het programma *smfmind* een opgestaarde C source te compileren (*smfmind*) en een sh op root beschikbaar uit te voeren via een bug in *fingerd*. Verder probeerde het systeem of er nog andere hosts op deze machine waren aangesloten, en zo ja dan werden ook deze geïndectreed. Om hostnames uit een directory te kunnen halen werden een groot aantal voor de hand liggende wachtwoorden geprobeerd (*rtshrewc*).]

THE CRACKDOWN:

Three main 'viral' teams from Berkeley, MIT and Purdue found copies of the VAX code (the .a files had all the symbols intact with somewhat meaningful names) and decompiled it into about 3000 lines of C. The BSD development team picked fun at the code, even going so far to point out bugs in the code and supplying source patches for it. They have not released the actual source code, however, and refuse to do so. That could change: there are a number of people who want to see the code.

Portions of the code appear incomplete, as if the program development was not yet finished. For example, it knows the offset needed to break the BSD fingerprint, but doesn't know the correct offset for Sun's fingerprint (which causes it to dump core); it also doesn't guess its tracks as cleverly as it might, and so on.

The close scrutiny of the code also turned up comments on the programmer's style. Verbalized from someone at MIT:

"From disassembling the code, it looks like the programmer is really really conservative about checking return codes, and, in addition, prefers to use array indexing instead of pointers to walk through arrays."

Anyone who looks at the binary will not see any embedded strings: they are XOR'ed with 81 (hex). That's how the shell commands are embedded. The "obvious" passwords are stored with their high bit set.

Although it spreads very fast, it is somewhat slowed down by the fact that it drives the load average up on the machines: this is due to all the encryptions going on, and the large number of incoming worms from other machines.

[Initially, the fastest defense against the worm is to create a directory called *haxfingph*. The script that creates *haxfingph* from one of the .a files checks to see if *haxfingph* exists, but not to see if it's a directory. This fix is known as 'the condom'.]

NOW WHAT?

Most Internet systems running 4.3BSD or SunOS have installed the necessary patches to close the holes and have regained the Internet. As you would expect, there is a renewed interest in system/network security, finding and plugging holes, and speculation over what will happen to the worm's creator.

If you haven't read or watched the news, various log files have named the responsible person as Robert Morris Jr., a 23-year-old doctoral student at Cornell. His father is head of the National Computer Security Center, the NSA's public effort in computer security, and has lectured widely on security aspects of UNIX.

Associates of the student claim the worm was a "mistake" — that he intended to unleash it but it was not supposed to move so quickly or spread so much. His goal (from what I understand) was to have a program "live" within the Internet. If the reports that he intended it to spread slowly are true, then it's possible that the bytes sent to arnie.berkeley.edu were intended to monitor the spread of the worm. Some news reports mentioned that he predicted when, via some "moving mechanism" he saw how fast it had propagated.

A source inside DEC reports that although the worm didn't make much progress there, it was sighted on several machines that wouldn't be on its normal propagation path, i.e. not gateways and not on the same subnet. Those machines are not reachable from the outside. Morris was a summer intern at DEC in '87. He might have included names or adding on to remembered as targets for infecting hidden internal networks. Most of the DEC machines in question belong to the group he worked in.

The final word has not been written — I don't think the FBI have even met with this guy yet. It will be interesting to see what happens.

~~~~~  
Article on the Internet worm

AL FASOLDT is a technology writer (syndicated newspaper columnist) and a radio writer (*Fischer Magazine*), newspaper editor in Syracuse, NY (the daily *Herald-Journal*), poet, bicyclist, computerist

who loves simple programming: a fan of the Atari ST and up to at all of MS-DOS computers; 3 grown children.

"Let's start things off with some thoughts on who is really responsible here."

This is an article I wrote for distribution this coming week.

AThis can be reproduced in electronic form as long as the text is not altered and this note remains on top. Distributed by the Technologic EBS.

By Al Fasoldt

There's an untold story in the hour over the electronic virus that infected 6,000 mainframe computers across the country earlier this month.

Left out of the many accounts of the prank pulled by a Cornell graduate student is something that could be the single most important issue of computer networking in the next decade.

It is put most simply in the form of a question: Who is in charge of our main frame computer network?

In more complete terms, it can be stated this way: Are we placing too much trust in the systems managers who run our nation's medium- and large-size computer systems?

I am posing the question for a practical reason, not a theoretical one. Lost in the hour over the mass electronic break-in is the fact that it could have been prevented — if the people in charge of the computers had been doing their job.

The hacker, Robert Morris, exploited a weakness in the operating system of the at computer systems. The weakness was known to the operating system's designers, and the company that supplies the operating system had long ago sent notices to all its customers explaining how to patch the operating system to fix the weakness.

All these thousands of systems managers had to do was read their mail.

Most of them didn't. Most of them ignored the plea from the operating system's designers to make the fix before someone broke into these computers through this weak area, called the "back door."

There is no other word for this than incompetence. Those who think it's unlikely that most mainframe computer systems managers are incompetent - at least in this one area, if in no other - have their heads in the sand.

Think of it in terms of human viruses. If doctors throughout the country were warned of a potentially dangerous new strain in a major drug and most of them did nothing about it, how long would we last? We would demand that the medical profession act immediately to remove those doctors who don't have enough sense to protect the public.

Are we going to do the same thing in regard to our systems managers?

I'm a realist. I know what the answer is. They'll go on protecting their jobs by making up excuses. They'll tell the people who hired them that the entire subject is too technical to explain, but they have the situation well in hand.

But. Every systems manager who ignored the warnings on the filter in Unix, the operating system that Robert Morris coded right through, should be fired.

It's as simple as that. It's time that we treated networked computer systems seriously. It's time that we stopped accepting the technobabble from these incompetents as something that no one else can comprehend. The rest of us can comprehend it just fine, thank you.

If you agree, mail a copy of this article to your boss. Send a copy to the person who hires and fires the systems manager in your company or university.

Send him a message before another Robert Morris sends them something else.

How can computers catch a virus? It's easy. Keep in mind that a computer works quite a bit like a human being. Both need a central processor to run properly - a CPU chip in one case and a brain and central nervous system in the other. And both need the correct programs to work right - an operating system in the computer and an autonomous set of instructions to the organs of the body in the human. Each one can get sick when a virus works its way into the system and throws it off stride. In both the computer and the human, the virus hides itself and alters the day-to-day operations of its host. In its mildest form, the virus merely slows everything down. The computer responds sluggishly, and the human feels weak and rundown. At its worst, the virus can make either type of host so sick that it may not recover without intensive care. So far, what we have been describing also characterizes a simpler form of intruder, called a worm. The difference between a worm and a virus is that worms don't create new copies of themselves, but viruses do; in fact, the strongest viruses in computers and humans can create new clones of themselves many times a minute. The major conceptual difference is that human viruses are actual creatures, and they can sometimes be seen under a microscope. But computer viruses are formless groups of numbers written as a program. This may make them seem less harmful than human viruses, but it would be a serious mistake for us to treat them that way.



## CCC vandaag

Al vroeg in de tachtiger jaren waren de Duitse hackers georganiseerd in de CCC. De CCC, ter breed van o.a. de grote NASA hack van vorig jaar en de uitgave van de Hacker Bible (waarschijnlijk 2 delen verkrijgbaar) stond vooral bekend als een Hamburger club. Hoewel dit in het begin van de jaren tachtig misschien ook zo was, is de werkelijkheid nu anders.

Hier in Nederland waren omstreeks 1985 slechts enkele mensen actief, en om dat zij geen club hadden opgericht is het hacken in die tijd tamelijk onroepelijk geweest. Nieuwe hackers konden alleen 'in de groep opgenomen worden' door te reukig frequente contacten met het groepje bekende hackers.

Ik in Nederland de 'vorkoers' (daarom nog tamelijk klein, in Duitsland zijn honderden hackers actief. Als je dan ook de enorme afstanden tussen de Duitse publiek bedijkt is het niet meer dan logisch dat er zich kleinere regionale hackgroepen vormen.

De belangrijkste onderscheiden tussen de CCC op een rijtje.

Hoewel de CCC in Berlijn is ontstaan heeft het zwaartepunt altijd in Hamburg gelegen. De groep in Berlijn is nooit echt georganiseerd geweest: veel contact met de rest van de CCC is er niet, en in ieder geval manifesteert het Berlijnse deel van de CCC zich niet echt als groep.

Hamburg is van oudsher het middelpunt van de CCC wereld. Het is het laatste paar worden belangrijke zaken ook door het Hamburgers georganiseerd. De scène werd dan ook zo groot dat ze geen niet meer vanuit een punt te organiseren was. Stefan Wernery en Wau

Holland (die nu in Heidelberg woont, daarover straks) hebben de bal hier aan het rolen gebracht, en het is niet meer dan logisch dat de 'macht' zich hier geconcentreerd had. Hoewel van Hamburg is het er nog steeds van overtuigd zijn dat Hamburg het magische centrum van de wereld is, lijkt de 'hackings' alleen het absoluut niet erg te vinden de macht aan de rest van de ERM over te dragen.

In Lüneburg, tegen de Duitse grens aan, manifesteert zich nu een nieuwe groep hackers. Deze hackers zijn goed georganiseerd en hebben duidelijke leden. Hoewel de rest misschien terecht moet dat de Lüneburgers 'Widernacht sterflich' georganiseerd zijn, ze moeten ook toegeven dat je ze een een bonderschap kunt denken. Als je daar op een bijeenkomst komt, dan komen er ook 20 mensen, er is discussie, eren en discussies, 'alles in orde'.

In München, bekend als de andere kant van de Bismarckpubliek, zitten hier een de afgeleefde Duiters een aantal kleine pragmatische hackers. Waar in het noorden nogal een grote problemen zijn rond zaken als het verzamelen van geld van de media doet men hier niet meer lijn de afgeleefde weten 'wat een merk waard is'. Wordt in de rest van het land toch in een underground achtige omgeving gebracht, de Müncheners hebben alle meestal een nette baan. Deze dank kunnen ze soms hard-niet uit de haak komen met bijvoorbeeld harde disk presenten aan het adres van Philips in de tijd dat Stefan Wernery in Frankfurt in de gevangenis zat. Toch is het wellicht op hetzelfde niveau als Hamburg, maar toch moeten we het geweten van de CCC elders zoeken...

En wat in Heidelberg: hier zitten Bernd Fox en Wau Holland een het hoofd van de rest oudere CCC'ers. Hier wordt niet gesproken, hier wordt nageacht over de toekomst van de informatie-

Samenwerking). De werkelijk maatschappijwetenschappelijke problemen komen dan ook veel al uit Hildesheim. Ook de verbanden met de Duitse politiek legt hier de Duitse Grünen zijn door de Hildesheimers medede het rapport "Tora kúnen computer dan da nicht (ontwinnen kunnen)" uitgebreid geantwoord over computers, informatie-maatschappij en wat daar nogal verder bij komt kijken. In Hildesheim moet ook de echte hacker-ethiek genoemd worden. Het is nu Steven Levy binnen en hier 'nauwkeurig'.

In Keulen was al heel vroeg een groep met mailboxes en netwerken aan het spelen. Technisch is deze groep zeer goed, maar hiermee hadden ze al te veel lol dat echte hacking hier nooit van de grond gekomen is. Deze groep heeft pas invloed gewonnen toen networking binnen de CCC belangrijk werd. Een van de mailboxes wordt door de Socialistische computerklub gerund.

Dan is er nog een vierende rond in de tijd in Bielefeld al een groep computerbruikers die op een geheel alternatieve manier probeert iets met de computer te doen. Hielden met het hele moderne gedoe weinig te doen, maar voelen zich in een groep alternatieve computergebruikers toch goed thuis.

## Conflicten

Binnen de CCC zijn ook de nodige conflicten. Deze zijn echter niet zo zeer tussen de regio's als wel tussen de leden en de top van de CCC. (Misschien is het conflict met München over de te harde uitspraken in de pers een uitzondering). De leden verwijten de top te publiciteitsgeil te zijn en te veel in de openbaarheid te treden. De top verweert zich door te zeggen dat het nodig is bepaalde zaken steeds weer onder de aandacht van menig mens te brengen. Ze zegt dat zij ook door veel leden zelf naar voren geschoven wordt omdat veel leden niet in de open-

baarheid willen treden. Van de leden is vaak ook harde kritiek op Stefan Werner te horen. Vooral toen hij probeerde zijn verantwoordelijkheid uit Frankfurt aan de hoogte blader te verlagen moest hij het zwaar ontgelden. Ditge leden dringen met opzeggens van hun lidmaatschap, maar het lijkt er op dat de zaak met een steun is afgeronden.

Ook binnen de top van de CCC zijn spanningen. Een van de huidige leiders is de ruide rond Jürgen Wiedeman. Jürgen is behalve hacker ook journalist en heeft meegewerkt aan 'Das Chaos Computer Buch'. Dit boek bevat behalve de geschiedenis van de CCC ook enige andere belangrijke in de kaders, en dat is Jürgen niet onverdeeld in dank afgenomen.

Hier is voor een Nederlandse hacker bezield een schrik om te zien hoe somber hackers daar tegenover elkaar staan. Jürgen belt naar de organisatie van het congres, hij heeft een auto nodig om heen met zijn spullen naar het congres te vervoeren. Een van de aanwezige te staatsleden wordt gevraagd Jürgen op te halen. "Wilde Jürgen?" vraagt hij. "Jürgen Wiedeman". "Nee, die mag ik niet, sorry, dat doe ik niet."

Voordat ik december vorig jaar in Hamburg was dacht ik alijd dat het beter was als we ook in Nederland niet in een groep organiseren, om dit soort problemen te voorkomen. Maar op het congres heb ik aan den lijve ondervonden hoe goed het is om iets van een organisatie te hebben. Samenkomsten kunnen gemakkelijker worden georganiseerd en de hacker/beweging is toegankelijk. Het bestaat niet langer alleen maar uit hele kleine hyperbomen bij mensen thuis, maar dan kunnen ook wat grotere dingen gedaan worden, zodat er meer mensen met hackers kennis kunnen maken.

RDP

# CHAOS COMMUNICATION CONGRESS '88

28-30 december 1988

Ik had in Amsterdam al kennis gemaakt met enige leden van de Chaos Computer Club toen ze hier waren voor een info-show in Paradiso. Toen ik dus hoorde dat er in Hamburg een congres georganiseerd was in de laatste week van december ben ik daar maar even heen bij gekomen.

De henneging bleef algeheel (met een laptop XT en een Canon X-49 handheld in mijn rugzak). 's Avonds had ik een afspraak in Hamburg, waar ik met Steffen heb afgesproken, en bij hem sloep ik ook gedurende het congres. Voordat we naar op hun gaan leden we op de plaatselijke brandweerlocatie eerst nog even een oude brandweermotor met een telefoon spelen, lichtprojector en dergelijke. Steffen zit bij de brandweer, en dit mag bijbrengen.

De volgende ochtend begint de voorbereiding voor het congres. Steffen en ik komen te laat aan bij het Fideletätter Bürgerhaus de hele club staat daar buiten te wachten omdat Steffen de sleutel heeft. Eerstmaal bliken 'Och's' lief. Telefoonkabels worden aangelegd, computers gaan stilstand etc. etc. Ook wordt een programma ingedicht waar mensen nodig kunnen werken aan artikelen over het congres. Men vraagt mij om bij de opening van het congres (vrijdag) iets te vertellen over hackers in Nederland.

Aan het eind van de dag is een groot deel van de techniek in orde en komen we weer lateraan na eerst het Hamburgse uitgaansleven van deeltijd te hebben bevroord.

De volgende ochtend volgt het laatste middag te zijn. Ik werk Steffen en die blijft graag te hebben. Als we om 15.00 aankomen in het Bürgerhaus is er weinig veranderd. Men loopt een beetje in het rond maar lijkt zonder Steffen dat de hele anders organiseert een beetje uit het hoofd gelopen.

Omdat er al maandag al zo veel gedaan is heeft er vandaag niet veel te gebeuren. Dat leidt er toe dat een groot deel van de aanwezige hackers spelletjes (al dan niet op andere computers) dit te spelen.

De laatste hand wordt gelegd aan het programma, het wordt duidelijk wat er zo al gaat gebeuren dit jaar. Hoewel echt duidelijk wordt dat op een Chaos Congress nooit. Het programma is hier niet anders, stelsel gegeven, maar een soort leidend organisatie elke ritueel veranderd er wel iets en het hebben van een up-to date print-out is een must.

Als vrijdag het congres begint kom ik pas om 12.30 aan. Presies op tijd, ik kan gelijk het tweed op. Wijn Holand opent het congres met een kort welkomwoord en dan kom ik als eerste spreker. Ik had echter nog geen tijd gehad om mijn tekst te configureren, en ook voor een print-out had ik geen tijd. Dus daar zit ik met de laptop voor me, halve leed is slecht Duits.

Als ik het heb over de gaten in autorisatiesystemen 1 die in Duitsland nog te veel kunnen worden blijft men mij enigzins ongelukkig aan. Pas later dringt het tot velen door dat de Duitse hackers hier individueel iets over het hoofd hebben gezien.

Dit blijkt van echter dat de hackers hier niet geloven in een taalbarrière ook al was je Duits erbarmelijk, men was men bereid nodig naar je te luisteren. Pas later realiseerde ik me dat dat natuurlijk ook kwam omdat ik meer hulp organiseer. Missen dat daar alleen maar de gaten

kwamen hebben bepaald doeltreffende overeenstemming met de toegenomen belangstelling van de organisatie (en een deel van de Duitse hacker).

Na de openings toespraak liepen de tel pas erin in de hack rooms werden adressen en NSA lijsten uitgeverdeeld, PAD's opgeleest, computers gedemonstreerd en ga zo maar door. Grote groepen mensen om sommige computers, waar dan op dat moment iets spannends gebeurde.

In de andere ruimten vonden in de drie dagen dat het congres duurde allerlei conferenties plaats. Een groep uit het aanbod UUCP, over het UUCP netwerk, PC DES over het DES coderingsproces en een zeer snelle PC implementatie daarvan, gesproken door Bernd Fox, die ook de conferentie leidde. De laatste was ergerlijk "Daaromheen in de Netwer". Onder deze titel zalge totel gaat een aantal problemen schuik als je meer informatie krijgt moet je steeds selectiever zijn. Wat doe je als 90% van de informatie berbaat uit teetherichtlijen etc?

In de posterkamer onderkussen probeer de men berichten over de loop van het congres de wereld in de krijgen. Een de toerleiding met DPA, het Duitse nationale persbureau, bewees goede diensten.

In de Markthalle, een maal aan de andere kant van Hamburg, waren ook een aantal zaken georganiseerd die een grote rol zal nodig hadden. Zo was er woenr dagvond het koninkrijk "Chaos en Computercult", gespeeld door een koninkrijkschap dat niets met de CEC te maken had, maar hacken gewoon wel een spannend onderwerp vond. Hiermed het ber dert niet onauddig wat kun je met zeggen dat de makers van dit stuk al te veel van der hebben ondervonden van kennis van zaken op hack gebied (gamerele netjes achterlatter die werden gepresenteerd als het nieuwste van het nieuwste en zo).

Donderdag vond er in de zelfde Markt halle een discussie plaats die het karakter

van het congres had. moesten woorden een confrontatie tussen Christian Lichte van de Verfassungsschutz (het ons BVD) en de CCC. Vooral over de criminalisatie van de CCC in Duitsland waar de Verfassungsschutz hand aan meewerkt voor het nodige gezegd zijn... Als Lichte gekomen was. Maar op het laatste moment werd telefonisch afgezegd om 'veiligheidsredenen'. Ook een telefoonschetsing was koninklijk voor de gezondheid van Lichte te gevaarlijk.

Na het afscheid van tegenpartij is toen een discussie op gang gekomen over de gevolgen van het nieuwe digitale telefoonnet ISDN, dat ook in Nederland in voorbereiding is. Met dit net kan veel makkelijker het belgedrag van mensen worden bekeken, zodat invoering van ISDN een afbreuk is op de privacy van telefoongebruikers.

Als het congres de volgende dag (vrijdag) wordt afgesloten liepen de mensen gaar uiteen. Wie verwacht had een goed georganiseerd congres met een maximum aan informatie aan te treffen moest bedrogen uit. Wie stil was op een familie treffen zat midden in de roos. Want door al die vervolgingen in Duitsland is de CEC een hechte vriendschaps geworden. Als je, met dit, het ontmoeten van leuke mensen ook belangrijk vindt dan is het Chaos Communication Congress '89 onmisbaar!



## BACKUP

Zie zeggen wel eens dat hackers slechte mensen zijn die systemen stuk maken. Het tegendeel is waar: wij helpen de arme systembeheerders door van belangrijke files in hun systeem een backup te maken. Mocht onverhoopt een hard-disk crash plaatsvinden dan kan de file eenvoudig uit het betreffende systeem van BLACK-TIC worden overgetikt (systeembeheerders hoeven geen copyright-gelden af te dragen).

Een Black-Tic leenarservice.

### CONFIDENTIAL

Peter,

Theo's salary level and grade have to far been entirely a matter for you to specify from Holland; obviously any future arrangements will still have to be agreed by you. My engineering staff would recommend from what we have seen of Theo so far that he should be graded at the US equivalent of an TYBE CD2 position, Grade 8 on the University of Pittsburgh scale. That is at the same grade as our most experienced technicians (three grades above our most recent hires) but two grades below our recently appointed electronics supervisor. If paid through the HUVT, Theo would therefore receive \$24,396 per annum. If Arny were right (we do not think so), Theo would be at Grade 10 at a salary of \$28,344 per annum. A compromise of grade 9 would yield a salary of \$26,436 per annum, almost exactly what you paid him in 1986. (According to our records he was paid \$18,329.30 plus \$7200 rent allowance plus \$1064 medical insurance contribution, total \$26,593 - slightly above

our grade 10). I would say that in view of the fact that Theo has tenure with you - whereas our grade 10s do not have tenure - that Theo's pay is already adequate to meet Arny's point of view, and that TRD can therefore expect him to work at his computer technician job, without any change in salary. This is a good job, involving training and the chance to develop his potential a great deal further. I would like, effective 1st July - when TRD takes over the management of Theo - that we manage Theo's career on the same operating basis as John Baker, and tell you in the same way as we tell you for John Baker's services. He would start at grade 9, with no initial change in salary (we would use the next cost of living increase due to HUVT employees to align things next to). Unfortunately, there are obvious complications in that Theo's conditions of service here presently include provision of house rental etc., and his job, unlike John's is (I presume) tenured. The HUVT positions do not include all these privileges. I have asked Donald van Diepen to see if we could arrange to have Theo's remuneration contributions paid directly to Holland by the TYBE, and have all other aspects of his job managed through the HUVT. I would assume that the Dutch authorities would retain all Theo's rights of tenure if we were to make an arrangement like this. Comments?

